AO 106 (Rev. 01/09) Application for a Search Warrant

SEALED

FILED
MAR 23 2016
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

UNITED STATES DISTRICT COURT

for the

Southern District of California

7/20/17
UNSEALED PER ORDER OF COURT

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Google, Inc, 1600 Amphitheatre Parkway, Mountain View, CA 94043
for account: cybercrimestoppers.dhls@gmail.com

Case No. 16MJ0872

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California *(identify the person or describe property to be searched and give its location):* see Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: see Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 912, and the application is based on these facts: See attached affidavit

☑ Continued on the attached sheet.

☑ ~~Delayed notice of 45 days (give exact ending date if more than 30 days:~~ 05/04/2016) is requested ~~under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.~~

Stirling A Campbell
Applicant's signature

Stirling Campbell, HSI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 3/22/16

Mitchell D. Dembin
Judge's signature

City and state: San Diego, CA

Mitchell D. Dembin, United States Magistrate Judge
Printed name and title

1 nbp

X6735
03/22/16

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Special Agent Stirling Campbell, upon being duly sworn do hereby state that the following is true to my knowledge and belief:

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI) having been so employed since April 2006. I am currently assigned to the Special Agent in Charge (SAC) San Diego Office, Cyber Crimes Group within HSI in San Diego, California. Prior to this time, I worked as a United States Customs and Border Protection Officer in Los Angeles and Long Beach, California for approximately two (2) years and two (2) months. I have a Bachelor's Degree in Economics from the University of California, San Diego. I have received training from the Federal Law Enforcement Training Center in the area of child pornography investigations and pedophile behavior. I have assisted in the service of numerous search warrants involving computer/cyber-crimes. I am currently assigned to the Internet Crimes Against Children (ICAC) task force in San Diego, California. This task force includes members of the San Diego Police Department, San Diego County Sheriff's Department, U.S. Postal Inspection Service, Federal Bureau of Investigations, Naval Criminal Investigative Service, U.S. Attorney's Office and the San Diego County District Attorney's Office. Throughout my tenure with HSI, I have participated in numerous investigations involving child exploitation, human trafficking, human smuggling, financial crimes and narcotics. As an HSI Special Agent assigned to the ICAC task force, I investigate criminal violations relating to child exploitation, child pornography and cybercrimes, including violations pertaining to impersonating an officer, in violation of Title 18, United States Code, Section 912, blackmail, in violation of Title 18, United States Code, Section 873, extortion through interstate communications, in violation of Title 18, United States Code, Section 875, mailing threatening communications, in

violation of Title 18, United States Code, Section 876, and receiving proceeds of extortion, in violation of Title 18, United States Code, Section 880 and conspiracy to commit these offenses, in violation of Title 18, United States Code, Section 371. As a federal agent, I am authorized to investigate violations of laws of the United States and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. In preparation of this affidavit, I have discussed the facts of this case with other law enforcement agents, including officers within HSI and the Office of Professional Responsibility (OPR).

2. This affidavit is made in support of an application for a warrant to search for and seize evidence related to potential violations of Title 18, United States Code, Sections 371, 912, 873, 875, 876, and 880, at the location described in Attachment A, for evidence described in Attachment B.

3. This affidavit is based upon information I have gained through training and experience, as well as upon information relayed to me by other individuals, including law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known concerning this investigation but have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence relating to potential violations of Title 18, United States Code, Sections 371, 873, 875, 876, 880, and 912, further described in Attachment B, is located at Attachment A.

4. Based upon the following information, I believe there is probable cause to believe that currently located within Attachment A there is evidence concerning potential violations of Title 18 U.S.C. Sections 371, 873, 875, 876, 880, and 912, more particularly described in Attachment B.

BACKGROUND ON GOOGLE AND GMAIL EMAIL ACCOUNTS

5. Google is a corporation that provides Internet services worldwide. Google's electronic mail service, Gmail.com, allows Internet Service Provider (ISP) subscribers to communicate with other ISP subscribers and with others through the Internet via email communication.

INVESTIGATIVE RESULTS

6. On or about August 17, 2015, the Joint Intake Center (JIC) received a complaint from an individual (hereafter referred to as V1). V1 stated he was contacted by an agent named Charles ROBERTS from HSI's Cyber Crime Center (C3)[1] in order to extort money from him. V1 stated that ROBERTS demanded five hundred dollars ($500) in order to mitigate a pending arrest warrant for V1. V1 sent $500 per ROBERTS' instructions via MoneyGram Reference Number 99283061. V1 said ROBERTS used the email address c3childexploitaiondivision@gmail.com [sic] and phone number (407) 731-7186.

7. On November 24, 2015, Senior Special Agent (SSA) James Grundy with HSI's Office of Professional Responsibility and I interviewed V1. V1 stated that

[1] C3 is a legitimate section under HSI. It is comprised of the Cyber Crimes Unit, Child Exploitation Investigations Unit, and Computer Forensics Unit. C3 delivers computer-based technical services to support domestic and international investigations into cross border crimes and provides training to federal state, local and international law enforcement agencies. However, agents have conducted searches and are not aware of an individual named "Charles Roberts" listed within HSI or C3 as an agent.

during the month of July or August, 2015, he corresponded over email with a person that he believed to be an adult female. He met this person through personals posted on Craigslist, a classified advertisements website.

8. V1 stated that approximately two (2) days after his communications with this woman he received a call from "911." When V1 answered, a male identified himself as "Charles ROBERTS," an agent assigned to the "C3 Child Exploitation Division" in Florida. ROBERTS accused V1 of soliciting a minor on Craigslist and viewing a photo of the alleged minor. ROBERTS claimed that he had an arrest warrant for V1 as a result of this violation. ROBERTS then detailed specifics about V1's employment. (V1 later deduced that ROBERTS likely gained knowledge of his employment by querying V1's phone number, which is linked to V1's professional profile on the website LinkedIn.)

9. ROBERTS told V1 that according to the C3 investigation, V1 had not been in trouble for prior violations. ROBERTS said, as a result, he spoke with a C3 supervisor who agreed to allow the warrant to be cleared if V1 promptly paid a five hundred dollar ($500) fine. ROBERTS emailed a copy of a "Warrant Purge" document to V1, reflecting what would be filed to nullify the warrant as long as the fine was paid. V1 recalled ROBERTS used a Gmail account with the words "c3" and "child exploitation" in the address. V1 stated the "Warrant Purge" displayed the DHS seal, a judge's name, legal jargon related to child exploitation and represented ROBERTS as an officer from the "C3."

10. ROBERTS directed V1 to a nearby Walmart and told V1 to use MoneyGram to send the funds, since MoneyGram was backed by the federal

government and equipped to send ROBERTS a secured payment. V1 completed the money transfer per ROBERTS' instruction. V1 stated that after he paid the fine, he then took a closer look at the "Warrant Purge" and realized there were spelling errors in the document and that it probably was a fake. V1 stated ROBERTS again tried to contact him to pay additional fines, but V1 demurred. V1 subsequently made the report of the extortion.

11. On November 24, 2015, V1 provided SSA Grundy and me a copy of the email V1 received from ROBERTS on Saturday, August 1, 2015, at 10:47 a.m. Pacific Standard Time (PST). ROBERTS used the email address c3childexploitaiondivision@gmail.com [sic] to send a document to V1. The document is noted with the words "Warrant Purge" and reflects a payment of $500. In summary, the "Warrant Purge" contains the DHS seal with the heading "IN THE DISTRICT COURT OF JUSTICE OF THE STATE OF California FIFTH DISTRICT." Within the body of the document, the investigating agent is identified as "detective CHARLES ROBERTS EMPLOYED AND SWORN IN UNDER THE C3 CHILD EXPLOITATION UNIT."

12. On or about November 24, 2015, SSA Grundy submitted a DHS Summons to T-Mobile US Inc., requesting all subscriber and toll information associated to phone number (407) 731-7186. On or about January 7, 2016, T-Mobile US Inc. responded to the DHS Summons and provided one file pertaining to the subscriber of phone number (407) 731-7186. The following information was provided by T-Mobile:

Subscriber Name:	Abdullah Raheem
Subscriber Address:	1708 Columbus Ave

	Neptune NJ 07753-4623
Subscriber Status:	C
Activation Date:	06-03-2015
Termination Date:	10-02-2015
Account No:	497508316

13. On December 11, 2015, I submitted a DHS Summons to Google, Inc., requesting all information associated to c3childexploitaiondivision@gmail.com. The summons was accompanied by a court order commanding Google not to disclose the existence of the DHS Summons. *See* 15MC1444.

14. On or about December 15, 2015, Google responded to the DHS Summons and provided one file pertaining to Google account-holder(s) identified as c3childexploitaiondivision@gmail.com [sic], with internal Reference Number 651819. The following information was provided by Google:

Name: Charles Roberts
e-Mail: c3childexploitaiondivision@gmail.com
Services: Gmail, Google Talk, Web History
Created on: 2015/07/26-20:50:56-UTC
Terms of Service IP: 64.45.224.30, on 2015/07/26-20:50:56-UTC
Google Account ID: 482292487891

15. On or about December 16, 2015, SSA Grundy submitted a DHS Summons to CenturyLink requesting all information associated to IP address 64.45.224.30 associated with the email address c3childexploitaiondivision@gmail.com [sic].

16. On or about December 18, 2015, CenturyLink responded to the DHS Summons via fax pertaining to the account-holder(s) identified with the IP address

64.45.224.30. The following information was contained in the file provided by CenturyLink:

Target Information:	64.45.224.30
Customer Name:	Denisha Bacote
Billing Address:	106 Brixham Ct Kissimmee, FL 34758-4135
Established:	12/04/2014
Disconnect Date:	09/14/2015
Status:	Cancelled

17. HSI Intelligence Research Specialist (IRS) Kyle Chase conducted computerized records checks to identify possible occupants of 106 Brixham Ct, Kissimmee, FL 34758. IRS Chase identified Ronnie MONTGOMERY as reporting his address effective April 27, 2015 as 106 Brixham Ct., Kissimmee, FL 34758. New Jersey Department of Motor Vehicle (DMV) records checks list MONTGOMERY's address as 1708 Columbus Avenue, Neptune, NJ 07753, the same address for Abdullah RAHEEM, the subscriber of phone number (407) 731-7186 who used the name "ROBERTS" to communicate with V1.

18. On February 16, 2016, SSA Grundy and I interviewed an additional victim (hereafter referred to as V2). V2 stated that he had been on the personals section of Craigslist in July or August 2015. V2 gave an account similar to V1 about how he initially began communicating with a person he believed to be an adult female and was then contacted by "Agent ROBERTS." "ROBERTS" identified himself as an agent with HSI's C3 and accused V2 of soliciting a minor.

19. V2 confirmed he had also spoken with "ROBERTS" on phone number (407) 731-7186 during the month of July or August, 2015. V2 stated that

"ROBERTS" had changed his phone number several times since their initial phone conversation. V2 stated thirty (30) minutes before meeting with SSA Grundy and me on February 16, 2016, he had spoken to "ROBERTS" on phone number (407) 613-9452. "ROBERTS" continued to identify himself as a Special Agent with Homeland Security and wanted to be apprised if any other Federal Law Enforcement Agencies were to ever speak with V2 concerning this issue.

20. During the interview, V2 provided SSA Grundy and me with an email that he received from "ROBERTS" on August 22, 2015, at 8:40 a.m. PST. The document is similar to the previously described "Warrant Purge" document that was sent to V1, although this Warrant Purge contains V2's name. I also observed that the document was sent to V2 using a new email address, cybercrimescenterc3@gmail.com.

21. V2 stated he also sent monetary transactions in the forms of Homeland Security "fees" and "fines" via MoneyGram at "ROBERTS'" request. Summons results from MoneyGram confirm multiple transactions sent by V2 to "ROBERTS" and picked up at a Wal-Mart in Kissimmee, Florida ("Kissimmee Walmart"). Open records checks reflect the area code (407) used by the two (2) previously-mentioned phone numbers associated with "ROBERTS" are based principally in Orlando, Florida, but also include all of Orange, Osceola, and Seminole counties. Kissimmee is a city located in Osceola County, Florida, where the Kissimmee Walmart is located and where MONTGOMERY resides.

22. On one specific occasion, V2 sent $600 on reference number 98041315 to "ROBERTS" on August 24, 2015. MoneyGram summons results reflected that

"ROBERTS" picked up the funds from the Kissimmee Wal-Mart on August 25, 2015.

23. On August 26, 2015, MONTGOMERY posted a self-produced video to Facebook account profile https://facebook.com/profile.php?id= 100008589613118 of him picking up $600 at a Wal-Mart instore MoneyCenter. MONTGOMERY speaks throughout the video and his voice can be distinctly heard.

24. MoneyGram summons results reflected that on January 2, 2016, and January 21, 2016, "ROBERTS" again directed V2 to send funds via MoneyGram. According to records from MoneyGram, the receiver of the funds was MONTGOMERY. On February 15, 2016, V2 was instructed by "ROBERTS" to send approximately $1,545 to DeAngelo BACOTE. The Kissimmee Wal-Mart surveillance tapes show MONTGOMERY accompanying BACOTE when the two picked up the money.

25. On February 18, 2016, V1 and V2 both identified MONTGOMERY's voice played from the video posted to the Facebook account as the individual they spoke with over the phone known to them as "ROBERTS."

26. In order to gain access to a Facebook account, individuals must enter their registered email address and a password in the Log-In screen. Once a person logs in, they are able to post comments, photos, and videos to their accounts. On March 16, 2016, I received summons results from Facebook. Facebook identified MONTGOMERY's registered email address as **abdullahraheem5@gmail.com.** Abudullah RAHEEM is the name of the subscriber for phone number (407) 731-

7186, who self-identified as "ROBERTS," and a resident of the same house as MONTGOMERY in New Jersey.

27. Summons results from Facebook also showed that MONTGOMERY frequently used IP address 64.45.224.30 from June 13, 2015, to September 7, 2015, to log in and out of his Facebook account. IP address 64.45.224.30 was also used to create and log in and out of c3childexploitaiondivision@gmail.com, the email used to send the "Warrant Purge" to V1.

28. On March 3, 2016, OPR SSA Jacqueline McBride made contact with MONTGOMERY at his residence at 106 Brixham Ct, Kissimmee, FL. MONTGOMERY told McBride that he and others lived at this residence. On March 11, 2016, SSA McBride identified "ROBERTS'" voice from a monitored consensual call between V2 and "ROBERTS" as likely MONTGOMERY's voice.

29. On March 9, 2016, I spoke with V3, who was identified through MoneyGram subpoena transactions. V3 gave a similar account as V1 and V2 about communicating with a woman he met through Craigslist at around the beginning of September. He was then contacted by an individual who identified himself as a special agent a day or two later. V3 sent a payment of $880 to Steven MILLER to quash an investigation for soliciting a minor. V2 was directed to put the phone number "(866) 347-2423" on the MoneyGram transaction. The phone number (866) 347-2423, also known as (866) DHS-2-ICE, is the official government phone number for the HSI Tipline, where the public can report suspicious criminal activity to ICE Homeland Security Investigations.

30. On March 19, 2016, V3 provided me a copy of the email V3 received from MILLER. It was dated Friday, September 18, 2015, at 8:19 a.m. PST. MILLER used the email address **cybercrimestoppers.dhls@gmail.com** to send a document to V3. The document is similar to the previously-mentioned "Warrant Purge" documents sent to V1 and V2 and reflects a payment of $880. In summary, this document contains the heading "IN THE DISTRICT COURT OF JUSTICE OF THE STATE OF CALIFORNIA FIFTH DISTRICT." Within the body of the document, the investigating agent is identified as "special agent STEVEN MILLER EMPLOYED AND SWORN IN UNDER THE C3 CHILD EXPLOITATION UNIT.

31. A few days later, V3 noticed multiple typographical errors in the Warrant Purge document and grew suspicious. V3 contacted the person he knew as STEVEN MILLER to point out the mistakes and follow up, but he never received a return call.

32. Warrants to Google have issued for c3childexploitaiondivision@gmail.com and cybercrimescenterc3@gmail.com. We have not yet received a response from Google.

ATTEMPTS TO OBTAIN DATA

33. The United States has not attempted to obtain this data by other means.

GENUINE RISKS OF DESTRUCTION

34. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically stored data can be permanently deleted or modified by users possessing basic computer skills.

INTERNET SERVICE PROVIDER (ISP)

35. Google is an Internet company, which, among other things, provides electronic communication services to its subscribers. Google's electronic mail service allows subscribers to communicate with others through the Internet. ISP subscribers access Google's services through the Internet.

36. Subscribers to Google may use screen names during communications with others. The screen names may or may not identify the real name of the person using a particular screen name. Although Google requires users to subscribe for a free account, Google does not verify the information provided by the subscriber for its free services.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

37. Federal agents and investigative support personnel are trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google are not. It would be inappropriate and impractical for federal agents to search the vast computer network of Google for

the relevant accounts and then to analyze the contents of those accounts on the premises of Google. The impact on Google's business would be severe.

38. Therefore, I request authority to seize all content, including electronic mail and attachments, stored instant messages, stored voice messages, photographs and any other content from the Google account(s), as described in Attachment A. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Google, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Google to make a digital copy of the entire contents of the accounts subject to seizure. That copy will be provided to me or any other authorized federal agent. The copy will be forensically imaged and the image will then be analyzed to identify communications and other data subject to seizure pursuant to Attachment B. Relevant data will be copied to separate media. The original media will be sealed and maintained to establish authenticity, if necessary.

39. Analyzing the data provided by Google may require special technical skills, equipment and software. It also can be very time-consuming. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications, which files may have been attached to electronic mail, do not store data as searchable text. The data is saved in a proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to

properly analyze recovered data increases dramatically.

40. Based on the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. The personnel conducting the segregation and extraction of data will complete the analysis and provide the data authorized by this warrant to the investigating team within ninety (90) days of receipt of the data from the service provider, absent further application to this court.

41. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize all electronic mails that identify any users of the subject account(s) and any electronic mails sent or received in temporal proximity to incriminating electronic mails that provide context to the incriminating mails.

42. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification, segregation and extraction of data within the scope of this warrant.

REQUEST FOR SEALING AND PRECLUSION OF NOTICE

43. This is an ongoing investigation of which the target is unaware. It is very likely, based upon the above, that evidence of the crimes under investigation exists on computers subject to the control of the targets. There is reason to believe,

based on the above, that premature disclosure of the existence of the warrant will result in destruction or tampering with that evidence and seriously jeopardize the success of the investigation. Accordingly, it is requested that this warrant and its related materials be sealed until further order of the Court. In addition, pursuant to Title 18, United States Code, Section 2705(b), it is requested that this Court order the electronic service provider to whom this warrant is directed not to notify anyone of the existence of this warrant, other than its personnel essential to compliance with the execution of this warrant until further order of the Court.

CONCLUSION

44. In conclusion, based upon the information contained in this affidavit, I have reason to believe that evidence, fruits and instrumentalities relating to violations of Title 18, U.S.C. Sections 371, 873, 875, 876, 880 and 912, as further described in Attachment B, are located in Attachment A.

Stirling Campbell, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
this 22 day of March 2016.

THE HONORABLE MITCHELL D. DEMBIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Records concerning **cybercrimestoppers.dhls@gmail.com** held by Google, Inc., an Internet Service Provider with its primary computer information systems and other electronic communications and storage systems, records and data located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

I. Service of Warrant

The officer executing the warrant shall permit Google, Inc., as custodian of the computer files described in Section II below, to locate the files relevant to Attachment A and copy them onto removable electronic storage media and deliver the same to the officer or agent.

II. Items subject to seizure

All subscriber and/or user information, all electronic mail, images, text messages, histories, buddy lists, profiles, method of payment, detailed billing records, access logs, transactional data and any other files associated with the following accounts and screen names:

cybercrimestoppers.dhls@gmail.com

The search of the data supplied by Google, Inc. pursuant to this warrant will be conducted as provided in the "Procedures for Electronically Stored Information" of the affidavit submitted in support of this search warrant and will be limited to seizing electronic mail and attachments that are evidence of violations of Title 18, United States Code, Sections 371, 912, 873, 875, 876, and 880 **from August 15, 2015 to September 30, 2015.**

a. Electronic communications and attachments (sent, saved or received) pertaining to the assuming or pretending to be an officer or employee acting under the authority of the United States or any department, agency or officer thereof, in violation of Title 18, United States Code, Sections 371, 912, 873, 875, 876, and 880.

b. Electronic mail and attachments related to the identities of any co-conspirators.

c. Electronic mail and attachments that provide context to any electronic mail reflecting the criminal activity described in this warrant including any electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail that identifies users of the subject account during the relevant period of time.

d. Electronic mail and attachments, which reflect that true identity of the user.